Секция «Международная безопасность»

Подходы США и КНР к обеспечению кибербезопасности

Малышев Александр Сергеевич

Студент (бакалавр)

Дальневосточный федеральный университет, Восточный институт - Школа региональных и международных исследований, Владивосток, Россия

E-mail: tikrong@mail.ru

Повсеместная информатизация привела к возникновению принципиально новой среды противоборства конкурирующих государств - киберпространства. И если вопрос о взаимоотношении государств в наземном, морском, воздушном и даже космическом пространстве чётко регламентирован в международном праве, то вопрос о взаимоотношении государств в киберпространстве остаётся открытым.

Сегодня мы видим, что акты кибератак и кибершпионажа приносят колоссальный ущерб экономикам стран, который исчисляется десятками миллиардов долларов [1]. Заместитель министра обороны США, Уильям Линн, в ходе одного из своих выступлений сказал: «В XXI веке биты и байты могут быть такими же опасными, как пули и бомбы»[2]. В связи с этим повышается научный интерес к проблеме кибербезопасности, так как по мнению многих аналитиков киберпространство может стать основной ареной для будущих войн. Поэтому в этой статье предлагается рассмотреть подходы к обеспечению кибербезопасности со стороны США, экономика которой наиболее зависит от киберпространства, и КНР, которую Вашингтон всё чаще обвиняет в посягательстве на интеллектуальную собственность и спонсирование кибератак. Кроме этого, представляется важным выявить причины и определить пути решения конфликтов в киберпространстве между этими двумя государствами.

После ряда крупных атак на американские серверы в начале XXI века, появились мнения, что США и Китай должны начать работать вместе над выработкой международного соглашения, касательно поведения стран в киберпространстве. Сторонники подобного соглашения утверждали, что у обоих стран есть общие интересы, так как Китай уже сегодня страдает от киберпреступности, а его зависимость от информационных технологий постоянно растёт.

Однако приходится признавать тот факт, что есть ряд трудностей, мешающих заключению подобного соглашения, и основная из них - фундаментально разный взгляд на информационное пространство и его защиту. США в своих официальных документах заявляют, что будут способствовать развитию открытого, взаимозависимого, безопасного и надёжного киберпространства, усиливая безопасность и поощрая свободу слова[3].

Китай, напротив, выступает за строгое регулирование интернета, опасаясь, что современные технологии связи могут способствовать росту нестабильности в стране. Они воспринимают попытки со стороны США преодолеть китайские интернет фильтры столь же опасными, как атаки хакеров на электростанции и другие стратегически важные объекты.

Эта разница во взглядах отражается и в концепциях безопасности. Если США под кибербезопасностью понимает обеспечение безопасности архитектуры интернета, то Китай смотрит на это понятие шире и называет его информационная безопасность, подразумевая ещё и контроль над распространением нежелательной информации. Эта разница в подходах представляет собой существенное препятствие на пути заключения межгосударственного соглашения по кибербезопасности.

Кроме этого, оба государства имеют свои цели в использовании киберпространства. Китай, считая себя более слабым с военной точки зрения чем США, вырабатывает страте-

гию асимметричного ответа. В качестве одного из её элементов выступает вмешательство в киберпространство потенциального противника. Например, оставляя следы после атак на электростанции в США или другие стратегически важные объекты, он предупреждает Вашингтон, что США не останутся неуязвимыми в случае потенциального конфликта.

Не вызывает сомнений, что многие кибератаки поддерживаются Пекином. Хорошо известно, что КНР стремится стать производителем инновационных продуктов с высокой добавленной стоимостью, а не производителем дешёвых товаров. Поэтому, помимо исследований, он прибегает к промышленному шпионажу, в т.ч. и кибершпионажу. Известны и случаи, когда Пекин прибегал к кибератакам для сохранения внутренней стабильности: в качестве примера могут служить атаки на информационные ресурсы тибетских активистов. И немаловажно, что на нападки и обвинения со стороны Вашингтона, КНР отвечает уличинеями США в неискренности и милитаризации киберпространства, посредством создания вирусов, подобных хорошо известному Stuxnet. Пекин убеждён, что США постоянно присутствуют во внутренних сетях Китая, что подтверждается недавними разоблачениями Эдварда Сноудена [4].

Учитывая разность в подходах определения кибербезопасности и наличие своих индивидуальных целей, можно предположить что так называемая кибервойна между США и КНР будет продолжаться. США будет продолжать улучшать обороноспособность своих серверов и повышать себестоимость атак для китайских хакеров. Скорее всего, Вашингтон продолжт взаимодействие со своими традиционными союзниками в регионе по выработке международных норм поведения в киберпространстве, которые усилят давление на Китай. Однако есть вероятность, что Китай будет работать в том же направлении и займётся экспортом своего видения кибербезопасности. Хорошим примером могут служить недавно достигнутые соглашения с Российской Федерацией по обеспечению безопасности национальных сегментов интернета, так как видение кибербезопасности у обеих государств становятся всё более близкими [5].

Подводя итог, можно отметить, что роль киберпространства возрастает с каждым годом. Всё больше и больше государств начинает уделять внимание защите киберпространства. Примечательно, что НАТО приравнивает кибератаку на члена союза к вооружённому нападению. Поэтому, возможно, вскоре тезис о том, что государство, контролирующее киберпространство, будет контролировать войну и мир, станет реальностью.

Источники и литература

1) Вести-Экономика [Электронный ресурс], Режим доступа: http://www.vestifinance.ru/articles/30226, свободный, Загл. с экрана
2) Русская служба BBC [Электронный ресурс], Режим доступа: http://www.bbc.co.uk/russian/international/2011/07/110714_pentagon_cyber_defence.shtml, свободный , Загл. с экрана
3) the White House [Электронный ресурс], Режим доступа: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, свободный , Загл. с экрана
4) Вести [Электронный ресурс], Режим доступа: https://www.vesti.ru/doc.html?id=1642063&cid=5, свободный, Загл. с экрана
5) Газета.ру [Электронный ресурс], Режим доступа: http://static.gazeta.ru/business/2014/11/24/6313205.shtml, свободный, Загл. с экрана